[The Guardian](https://www.theguardian.com/international)



*Lauri Love outside Westminster magistrates court, London, in July 2016. Photograph: Justin Tallis/AFP/Getty Images*

**Keyboard warrior: the British hacker fighting for his life**

***Lauri Love is charged with masterminding a 2013 attack by Anonymous on US government websites. Will Britain allow him to spend the rest of his days in an American prison?***

*by* [*Simon Parkin*](https://www.theguardian.com/profile/simon-parkin)

*Friday 8 September 2017 06.00 BST*

In October 2013, Lauri Love was drinking coffee in his dressing gown in his bedroom at his parents’ house in the village of Stradishall, Suffolk, when his mother called upstairs to say there was a deliveryman at the front door. Love, whose first name is pronounced “Lowry”, like the English painter, clomped downstairs. In the front doorway was a man dressed in a UPS uniform. “Are you Lauri Love?” the man asked. “Yes,” Love said. In a single motion, the man grabbed Love’s arm while presenting, not a package, but a pair of rattling handcuffs.

For the next five hours, while dusk turned to evening outside, Love, then 28, and his parents sat in the front room as a dozen or so men from the National [Crime](https://www.theguardian.com/uk/ukcrime) Agency, which investigates organised crime and other serious offences, checked the computers in the house. In Love’s bedroom, they found two laptops, and a PC tower humming on his desk. Among the bewildering Rolodex of open tabs in Love’s internet browsers, the officers found accounts logged into several hacker forums and arcane internet chatrooms. Downstairs, Love, who knew that anything said in these limbo moments of investigation could be later used against him, kept the conversation to small talk about the weather and football.

A little before midnight, Love was told that he was being arrested on suspicion of offences under the 1990 Computer Misuse Act, which covers, among other things, criminal hacking. He was not informed of what crimes he had allegedly committed, and was pressed into the back of an unmarked car, and driven to the police investigation centre in Bury St Edmunds. Love’s computers, along with USB drives and old computing hardware, much of which belonged to his father, a computing enthusiast, left, too. Love, who was subsequently diagnosed with Asperger syndrome – a form of [autism](https://www.theguardian.com/society/autism) that causes him to fret and obsess – did press-ups in his cell until, in the early hours of the morning, he fell into a brief and fitful sleep.

Later that day, still without any clear indication of what he was supposed to have done, Love was released with pre-charge bail conditions that he surrender his passports (one British, one Finnish) and agree to only access the internet while using his real name. When the family arrived home, they found reporters camped in their garden. What did the journalists know that the Loves did not? The answer came the following day: as Love was lying facedown on his bed, he heard a Radio 4 bulletin state that the son of a Suffolk vicar had been charged for hacking into computers belonging to the US government .

In fact, Love had not yet been charged with anything and, in October 2014, 12 months after his initial arrest, the Crown Prosecution Service announced that it no longer intended to prosecute. Love’s bail was cancelled and, for a moment, it seemed as though he was free – the victim, perhaps, of an international misunderstanding or a bungle. Then, in July 2015, Love was rearrested by the Metropolitan police, and spent a night at HMP Thameside, a Serco-run prison in south-east London, before being returned to his parents’ house. This time, Love’s pursuer was not the British criminal justice system, but the US government, which accused him of helping to orchestrate and wage cyber-attacks on official websites including those belonging to the Federal Reserve, Nasa and the US army between 2012 and 2013. Love, they claim, along with three other unnamed co-conspirators in Australia and Sweden, stole sensitive military data and personal information belonging to more than 100,000 government employees. He is wanted for crimes including conspiracy, fraud and identity theft in no fewer than three judicial US districts – the Southern District of New York, New Jersey, and the Eastern District of Virginia – a record unmatched by any foreign or domestic terrorist (but by at least one other hacker).

Love has not protested his innocence – he only points out that, without seeing the evidence, which the US Department of Justice refuses to reveal until he is on US soil, he cannot say one way or the other. But he had the means, motive and opportunity to carry out the crimes of which he stands accused. Even if Love is guilty, however, there are important legal and moral questions about whether he should be extradited to the US – a nation that has prosecuted hackers with unrivalled severity, and one where Love could be sentenced to spend the rest of his life in prison.

Four years after his initial arrest, Love has nearly exhausted his legal options. His extradition to the US is now perilously close. In September 2016, a district judge [refused to block](https://www.theguardian.com/commentisfree/2017/jan/09/lauri-love-justice-us-uk-courts-hacking-case-extradition)Love’s deportation. His remaining hope for mercy is a final appeal against extradition in the high court in November.

Love’s hope is for a full and fair trial in Britain. Even if he is found guilty in a British court of the most serious crimes in the US government’s indictment, his legal team estimate that he faces just a few months in prison. Failure means Love will be flown to a holding facility in New York, placed on suicide watch and probably forced to take antidepressants, prior to a trial. If he refuses to accept a plea deal and is convicted, he will face $9m (£6.8m) in fines and, experts estimate, a prison term of up to 99 years, a punishment illustrative of the US’s aggressive sentencing against hackers under the controversial [Computer Fraud and Abuse Act](https://www.theguardian.com/commentisfree/2013/mar/20/computer-fraud-abuse-act-law-technology).

To his supporters, Love’s case is crucial in establishing a precedent to prevent the US government from pursuing disproportionate and unjust claims against hackers, particularly on foreign soil. “Lauri’s case is critically important in determining the reach of America’s unusually harsh punitive sanctions for computer crimes,” says Naomi Colvin, who works for the Courage Foundation, the human rights group providing Love with legal support (its other seven beneficiaries include the whistleblowers [Edward Snowden](https://www.theguardian.com/us-news/edward-snowden) and [Chelsea Manning](https://www.theguardian.com/us-news/chelsea-manning)).

Furthermore, the case will illustrate the extent to which British judges now consider human rights when assessing deportation claims. Love’s defence team argues that the US prison system is unable to provide their client, who suffers from depression and bouts of untreatable eczema, with a basic level of care to meet his physical and mental health needs. “It’s difficult to see how anyone can be so obviously under the threat of suicide and yet we would still extradite,” says Karen Todner, Love’s UK lawyer. “To extradite would be horrendous; It would make a mockery of the [Human Rights Act](https://www.theguardian.com/law/human-rights-act).”

“I will kill myself before I’m put on a plane to America,” Love tells me. “They can use as much violence against me as they want, but my will is sovereign over my body and my life.” Yet the stakes are not only high for Love. Following the publication of an FBI report showing that Russian government-sponsored [hacking groups interfered with the 2016 US presidential elections](https://www.theguardian.com/technology/2017/jun/05/russia-us-election-hack-voting-system-nsa-report), the US appetite to make examples of foreign hackers has only intensified. Hacking, once viewed as a kind of prank carried out by wayward geeks, is now seen as a crucial weapon by foreign governments and organised crime. “The US must make every possible effort to pursue [Lauri Love],” says Michael Smith, a cyber-terrorism expert who provides consultancy to members of Congress and the National Security Council. “They must do everything in their powers to deter others from engaging in the same activities Love is accused of undertaking against the US government.”

\* \* \*

**On the evening of Friday 25 January 2013,** hackers who had [broken into the website](https://www.theguardian.com/technology/2013/jan/26/anonymous-hacking-takes-down-sentencing-commission-website) of the US Sentencing Commission, which sets guidelines for sentencing in US federal courts, took down the site’s front page and replaced it with a 10-minute YouTube video. The video, narrated in the detuned Stephen Hawking-esque computer voice favoured by soapboxing hackers, declared a cyberwar against the US judicial system for departing from “the noble ideals in which it was born and enshrined”. The long list of complaints in the video centred on the “disproportionate persecution” of hackers by prosecutors operating “in the interests of oppression or personal gain”.

Responsibility for the cyber-attack was claimed by a group connected to [Anonymous, the disparate hacktivist collective](https://www.theguardian.com/technology/anonymous) best known for its ideologically motivated pranks and rictus-grinning Guy Fawkes face masks. The group also claimed to have infiltrated a host of other government websites and collected troves of sensitive data. That information, which Anonymous did not specify, other than to claim it contained “secrets”, was then packaged up in a series of password-encrypted files (each named after a different US Supreme Court justice) and quietly uploaded to the internet. It was a digital ransom note: meet our demands for judicial reform, or we will release the password to the sensitive documents “We have not taken this action lightly, or without consideration of the possible consequences,” the authors said. “It is our hope that this warhead need never be detonated.”

News of the hack quickly spread. “Anonymous hackers target US agency site,” [stated one BBC headline](http://www.bbc.co.uk/news/world-us-canada-21213793). By the end of the weekend, the video had been viewed more than 1m times, with the US Sentencing Commission website repeatedly collapsing due to the vast amount of traffic it was drawing. On the Sunday, the hackers added an Easter egg: visitors who entered a classic video game cheat code were treated to a version of the arcade game Asteroids. (Shooting at the webpage revealed the text: “We do not forgive. We do not forget,” along with an image of the Guy Fawkes mask.)

It took the government a week to close whatever backdoors the hackers had used – the website now read, simply, “under construction” – but it had not been able to contain the embarrassment. “Feds stumbling after Anonymous launches Operation Last Resort”, a [tech blog](http://www.zdnet.com/article/feds-stumbling-after-anonymous-launches-operation-last-resort/) teased. The US government had been made to look amateurish during a high-profile game of cat-and-mouse, and news outlets had amplified the embarrassment.

According to the FBI, Love, who has been a skilled computer programmer since childhood (“When I look at computer code it’s like all I can hear is static,” Love’s father, Alexander, a prison chaplain, told me. “Lauri looks at code, he can hear the music”) was one of the leaders of the hack. In the months before the attack, an agent monitoring an online message room frequented by Love allegedly saw him describing the vulnerabilities of various US government websites.

*[](https://www.theguardian.com/news/2017/sep/08/lauri-love-british-hacker-anonymous-extradition-us%22%20%5Cl%20%22img-3)*

*A screenshot of the website of the U.S. Sentencing Commission after it was hijacked by the Anonymous in January 2013. Photograph: AP*

This was not news. In 2012, several months before the Anonymous hack, Chris Gates, a computer security expert for Uber in Washington DC, highlighted vulnerabilities in the US government’s website infrastructure at a conference in Boston. Gates even uploaded slideshows identifying which specific sites were vulnerable. According to the FBI, Love was recorded chatting to other hackers about stealing credit card details, although US prosecutors have not specified who was being targeted, how the numbers would have been harvested, or whether this was connected to the website hacks. Love’s braggadocio was, however, clear. In one exchange, he allegedly said: “You have no idea how much we can fuck with the US government if we wanted to.”

By the time their video went live, the Anonymous hackers had been illegally collecting data from US government websites for several weeks. The unauthorised access was allegedly gained by exploiting vulnerabilities in Adobe ColdFusion, software designed to build and administer websites and databases that is notoriously riddled with weak points. The trigger for the public attack, however, was much more recent: the highly publicised death of the US computer programmer and [hacktivist Aaron Swartz](https://www.theguardian.com/technology/aaron-swartz) 15 days earlier. Swartz [killed himself](https://www.theguardian.com/commentisfree/2015/feb/07/aaron-swartz-suicide-internets-own-boy) in his New York flat on 11 January while awaiting trial for alleged computer crimes. Those crimes were, his supporters claim, negligible and perhaps even justifiable. In late 2010, Swartz entered a utility closet at the Massachusetts Institute of Technology, hooked a laptop up to the university’s servers and set it to download more than [4m documents](https://www.theguardian.com/technology/2011/jul/19/reddit-founder-swartz-jstor-accused) from JSTOR, a database of academic journals that had been criticised by information activists for its prohibitively high access fees.

Love first heard about Swartz in 2001, when Swartz was working with the World Wide Web Consortium – the group, founded and led by [Tim Berners-Lee](https://www.theguardian.com/technology/timbernerslee), that sets the standards for the internet. Love was instantly beguiled. He saw Swartz as a pioneering visionary, building and fighting for a free and open internet. The following year, when Love was 17, he joined Swhack!, an internet chat channel founded by Swartz as a place to discuss everything from ideas to improve the internet to poetry, philosophy, linguistics and [artificial intelligence](https://www.theguardian.com/technology/artificialintelligenceai). While Love was involved in neither politics nor activism at the time, he says that Swartz’s ideology began to shape his philosophy deeply. “I started to see the power of the internet to make good things happen in the world.”

Following his arrest, federal prosecutors pursued Swartz with the same zeal with which they now pursue Love. Swartz was indicted on a raft of charges that carried a potential jail sentence of 35 years, even though neither JSTOR nor MIT pressed charges. The main prosecutor in the case, Stephen Heymann, went so far as to liken Swartz to a rapist. Swartz’s supporters pointed out he had not technically hacked anything – he had legally accessed the JSTOR database, in part to make a point about the public distribution of academic research, much of which is publicly funded. “The act was harmless,” [Tim Wu, a law professor at Columbia University](https://www.theguardian.com/technology/2017/jan/08/tim-wu-interview-internet-classic-party-went-sour-attention-merchants), wrote at the time. “JSTOR suffered no economic loss.”

Many hackers, including Love, believe Swartz was targeted for retribution by the US government. Swartz was the co-author of DeadDrop, software that allows whistleblowers to send sensitive documents securely to journalists – now used by media outlets around the world [under the name SecureDrop](https://securedrop.theguardian.com/). “The secret service had a grudge against him,” Love said. Swartz’s software appeared at a moment when US authorities had suffered a series of embarrassments at the hands of whistleblowers. “He was ‘caught’ downloading these journal articles when the US government had just got Chelsea Manning,” Love told me.

Love describes the day he heard the news of Swartz’s death as one of the darkest in his life. “I screamed,” he tells me. “I cried a lot. I shouted at the internet.” Once that initial shock dulled, Love’s disbelief began to darken into anger – directed at the prosecutors that he regards as Swartz’s murderers. “That the United States criminal justice system did not tie the noose around Aaron’s neck themselves is immaterial,” he says.

Love will not confirm or deny his participation in Operation Last Resort, although he tells me that he sees those who pursued Swartz as “self-interested prosecutors”, men and women with political aspirations trying to “put notches on their belt”. The US Army Investigation Command, for its part, claims to have traced the attacks to Love through an IP address in Romania, allegedly paid for via a Paypal account registered to a gmail account registered in his name.

On 27 February 2014, a little more than a year after the Anonymous hack and four months after Love’s initial arrest, Preet Bharara, then the attorney for the Southern District of New York, accused Love of having played an instrumental role in the attack. “Lauri Love is a sophisticated hacker who broke into Federal Reserve computers, stole sensitive personal information, and made it widely available, leaving people vulnerable to malicious use of that information,” he said. George Venizelos, FBI assistant director-in-charge of the New York office, said: “Fortunately, Love underestimated the level of sophistication and dedication maintained by the FBI Cyber Division” – his swagger matching his target’s alleged online comments about the US government.

\* \* \*

**The allegations against Love came at a sensitive time** for the US government, following a string of high-profile cases involving information leaks by politically motivated hackers. Four months prior to Love’s initial arrest, Manning had been sentenced to 35 years in prison for leaking nearly 750,000 classified or sensitive military and diplomatic documents. (She has subsequently been [pardoned](https://www.theguardian.com/us-news/2017/jan/17/chelsea-manning-sentence-commuted-barack-obama).) It was the same year that Matt DeHart, the former US Air National Guard intelligence analyst who claimed to have documents related to CIA misconduct, tried to flee the US and find asylum in Canada (he has subsequently agreed a plea deal). And it was a few months after [Barrett Brown](https://www.theguardian.com/profile/barrett-brown), a US journalist with ties to Anonymous, was arrested for a string of alleged offences related to the distribution of sensitive information – although most of the charges were dropped in 2014.

In each case, the US government pursued its targets with threats of wildly punitive sentences, often in search of plea bargains that would drastically reduce the sentence in exchange for an admission of guilt. “The prosecutorial culture is to aggressively pursue – this has been true since the first hacker trials almost 30 years ago,” says James Lewis, a cybersecurity expert at the Center for Strategic and International Studies in Washington DC. “It’s standard operating procedure for this kind of hack.”

The Computer Fraud and Abuse Act, which, put simply, prohibits unauthorised access to protected computers and networks, was first used in 1989, three years after its introduction, to indict Robert Morris Jr, son of the then-chief scientist at the NSA’s National Computer Security Center. Morris, who was then a Cornell graduate student, was sentenced to three years’ probation and 400 hours of community service for creating and distributing the [Morris worm](https://www.theguardian.com/technology/2010/sep/21/internet-worms-twitter), a piece of software that would slow down a computer to the point where it became unusable.

Morris, who is now a tenured professor at MIT, received a more lenient sentence than the hundreds of hackers who have subsequently been prosecuted under the act. The law’s loose definition, its critics argue, has been stretched far beyond that which lawmakers intended, allowing the full force of criminal law to be used against petty pranksters and digital vandals – usually those who challenge power, either through the causes they espouse, or because their actions cause embarrassment to those in authority. One civil liberties group campaigning for reform of the act describes it as “infamously problematic”.

In 2012, for example, the act was used to prosecute the hacker and neo-Nazi troll [Andrew Auernheimer](https://www.theguardian.com/technology/2014/apr/11/andrew-auernheimers-weev-conviction-vacated-hacking), better known as Weev, for accessing unprotected data that was freely available on an AT&T website. In 2013, the journalist Matthew Keys was indicted with providing a member of Anonymous with login credentials that granted access to edit the website of the Los Angeles Times. Only one headline was altered – a prank that was quickly rectified – yet Keys faced up to 25 years in prison under the act (he was sentenced to two).

As a result, British hackers who are charged with breaking into US computer systems are understandably eager to be tried in the UK. At least 12 individuals have been successful in this aim, including Mustafa Al-Bassam and [Jake Davis](https://www.theguardian.com/profile/jake-davis), who are both avid supporters of Love.

Tor Ekeland, the attorney who represented Auernheimer and Keys, and now represents Love, has called the act “a poorly written statute that doesn’t effectively define the main thing it seeks to prohibit”, namely the precise definition of unauthorised access. “There are ambiguities surrounding that definition that allow prosecutors wide latitude to bring charges under theories that shock computer people in the infosec [IT security] community.”

Love’s first dalliance with the hacking community came in his early teens, when he retreated online and fell in with a clandestine yet benevolent hacktivist organisation called the Cyber Army. They were simpler times, before hacking, be it for fun or resistance, was complicated by its associations with cruelty, snark and the racism that has flowered in online forums such as 4chan and Something Awful. The Cyber Army was intended to be a wholesome club for promising young computer programmers, although Love admits that its members would often deface websites to show off their talent. The group had a military-style hierarchy, and Love, who once laid telephone extension cables under the family’s carpets so that he could connect to the internet without his parents knowing, soon reached the rank of general. “It was all relatively boy scout-y stuff compared to what I got involved with later,” he says.

During this time, Love says he became more involved with Anonymous, which was evolving from a loosely coordinated, dispersed group of internet pranksters to something more organised and political. One of the group’s earliest targets was [the Church of Scientology](https://www.theguardian.com/world/scientology), whose well-documented attempts to suppress information via high-stakes legal cases typify the kind of institutionalised abuses of power that now fuel Anonymous’s activism. Love became involved in low-level attacks, tying up the church’s fax machines with a cascade of black pages.

The activism moved from the digital realm to the physical after Love joined Glasgow University in 2011 to study physics and computer science. There he became committed to a seven-month sit-in protest staged against funding cuts and rising tuition fees at the university. “My problem is I jump into things and get completely engrossed because of my Asperger’s,” he tells me. “It gave an immediate sense of having done something meaningful; I completely neglected my academic studies.” Early into the sit-in, 60 Strathclyde police officers in full riot gear and supported by a dog unit and a helicopter were called in to shunt the protesters out of the building. It was, one participant recalled, a traumatic event, and the police’s heavy-handedness may have hardened Love’s attitude to authority.

Love became increasingly committed to political causes (at the time, his Twitter screen name was “Smedley Butler”, after a major-general in the US Marines famous for his 1935 book criticising US foreign policy, War Is a Racket) but the activism took a toll on his physical and mental health. In his second year of study, Love was evicted from his shared flat in Glasgow following a drug bust in which a small quantity of cannabis was found in a sofa. He called home to ask that his family come to collect him. “I broke down in tears thinking that I had thrown away my life again,” he says. Back in Suffolk, directionless and without a focus for his political energies, Love fell into a bout of depression. A few months later, he heard about Swartz’s death.

\* \* \*



*A protester at the Million Masks March in Parliament Square, London, organised by Anonymous in November 2015. Photograph: Jack Taylor/AFP/Getty Images*

**Love’s** [**extradition hearing**](https://www.theguardian.com/law/2016/sep/16/computer-activist-lauri-love-loses-appeal-against-us-extradition) **took place** at Westminster magistrates court on a grey London day in September last year. Love was surprised, he tells me, at what he perceived to be the laissez-faire attitude of the prosecution team, which had seemingly prepared little material. “We were certain that we were going to win, as much because of how little effort the other side put in as anything else.” Love’s defence team, by contrast, called numerous expert witnesses to build a careful case, based on legal precedent.

The defence team’s argument hinged on the idea that to extradite Love to the US would be a denial of his human rights. They argued that US federal prisons such as Metropolitan Detention Center, Brooklyn, to which Love would be transferred, are unable to meet the needs of someone with acute Asperger’s. (The prison did not respond to requests for comment.) Simon Baron-Cohen, the director of Cambridge University’s Autism Research Centre, who first diagnosed Love with Asperger syndrome in 2015, was called as an expert witness. When the pair first met at the Courage Foundation’s office, Baron-Cohen tells me, Love had “hundreds, possibly thousands” of bookmarks and tabs open on his laptop. During his assessment with Baron-Cohen, Love scored 32 out of 50 on the Autism Quotient. Only 2% of the general population score this highly.

In the trial, Baron-Cohen explained that Love was likely to be unable to cope with the noise levels in a US prison, or away from the support of his family. After the Loves moved to Lowestoft, when Lauri was 16, the stress of the upheaval caused his hair to fall out. Later, he was twice hospitalised due to infections caused by his eczema. During his bouts of depression, Love says, he can consider suicide as often as four times a week.

The prosecution, meanwhile, called into question Love’s autism and mental health diagnoses, claiming that his conditions were either faked or exaggerated. “He needs a better story,” Lewis tells me. “There’s a long tradition of mobsters in the US discovering ailments after arrest, going to court in their bathrobes and so on. The Feds have seen it all. If it was a state court, I’d advise him to announce that he has found God, carry a bible and shout ‘Hallelujah’ – but this is a federal case, so he won’t get much sympathy.” (“I find that suggestion offensive,” Baron-Cohen tells me.)

“I am going to extradite Mr Love,” said the district judge Nina Tempia in her summary. Love sat impassively in the dock while his mother put her head in her hands. A gasp went up in the public gallery. “The judge did not reject his mental health issues,” Alexander Love tells me, a few months later. “The working was right but she gave the wrong answer.” Following the judgment, more than 100 MPs signed a joint letter to Barack Obama in his final month in office, asking that any criminal proceedings against Love take place in Britain. The US administration did not respond. Now, the only thing standing between Love and a US trial is the high court appeal.

Even if Love is guilty of all the charges against him – retributively breaking into flimsy US government servers, copying sensitive information and discussing with others what might be done with the haul – how could a life sentence fit a crime that cost not one person one cent?

“It’s an invitation to dance, and it’s a shame Love didn’t figure that out,” Lewis says. “Most governments generally disapprove of people breaking into military facilities but the grave sentence is also a negotiating tactic. The Department of Justice always starts with something draconian and the actual sentence ends up with community service or a few months wearing orange in a minimum-security prison.” But Love’s decision to fight the extradition – instead of pleading guilty in exchange for the promise of a lighter sentence in US prison – “may have taken these options off the table”, Lewis says.

Love believes the explanation may be even simpler. “Being hacked is great for creative accountancy,” he told me. According to Love, at the US Department of Energy, one of the victims of the alleged hacks, employee details were stored in a database that was 20 years out of date. “They had plans to fix this, like, a decade ago, and they just hadn’t been actioned.”

In effect, the US government is likely to assess damages – perhaps up to $60m, Love claims – according to what it would cost to shore up the pre-existing security holes that Love is accused of exploiting. “Nothing has to be substantiated,” Love says. Ironically, governments and companies often offer huge “bug bounties” to hackers who expose similar weaknesses in their technology. “They will happily pay people to get that same information that they found out from this alleged compromise,” he says.

It wasn’t supposed to be like this. In 2012, after facing widespread criticism, Theresa May – then the home secretary – [withdrew a 2006 order](https://www.theguardian.com/law/2012/oct/16/gary-mckinnon-theresa-may-human-rights) to extradite the autistic Scottish IT worker Gary McKinnon, who was accused of hacking into nearly 100 US military and Nasa computers in 2001 and 2002. McKinnon, who claimed he was searching for hidden evidence of UFO activity, allegedly deleted critical files from US government computers and posted a message reading “Your security is crap” on a US military website.

May still appears to view her decision as a legal triumph; she referenced the case in her first speech as prime minister, saying: “I was told I couldn’t stop Gary McKinnon’s extradition, but I stood up to the American government and I stopped it.” But after blocking McKinnon’s deportation, she moved to amend UK extradition law to introduce a “[forum bar](https://www.theguardian.com/politics/2013/feb/06/home-secretary-overhauls-extradition-laws)”, in which judges may rule that the US is not the proper forum for a trial if the alleged criminality largely took place in Britain, or if the suspect is particularly vulnerable. Critics, however, argue that the forum bar was principally a ploy to absolve any home secretary from having to get their hands dirty in this kind of internationally sensitive situation. Indeed, following Love’s initial court case, the current home secretary, Amber Rudd, wrote him a letter [claiming that her hands were tied](https://www.theguardian.com/law/2016/nov/14/amber-rudd-approves-lauri-love-extradition-to-us-on-hacking-charges).

The forum bar is yet to be successfully argued in any legal case. Todner, the London lawyer who has represented both McKinnon and Love, tells me that “the general attitude of judges is that the extradition treaty overrules the forum bar”. If this is the case, then the legislation is not worth the vellum on which it is written.

The November appeal of Love’s extradition will be the first – and likely final – substantive test of May’s forum bar. “If the forum bar doesn’t work for me, it’s hard to see how it could ever work to protect anyone,” Love says. Todner agrees: “If it succeeds then the UK police will have a green light to take more prosecutions here and not bow to the US pressure to extradite.” And if it fails? Many more British people will face extradition to the US, where they will find, as Colvin puts it, “long prison sentences, horrible prison conditions and plea bargaining”.

Love, meanwhile, waits. The University of East Anglia has suspended his studies in electrical engineering, pending the outcome of the extradition hearings. (“Immoral,” Alexander Love tells me. “You don’t rob someone on the basis of something that might happen.”) The university’s decision is especially painful in the knowledge that, had Love been allowed to stand trial in the UK following his initial arrest, and had he pled guilty to every charge, he would have spent a maximum of 18 months in prison. “It’s a particularly vindictive way they have gone about all of this,” Alexander Love says. “No evidence has been disclosed. No harm has been done. But they obviously feel that they want to make Lauri a deterrent. If you mess with us, they’re saying, this is what we can do to you.”

\* \* \*

**At a picnic bench in a clearing in Nutley Forest** in East Sussex, on an agreeably warm June afternoon, Love leans over a battered laptop pocked with stickers. (“Don’t feed the Google”; “Leak more docs”.) After a moment of frustration, he hisses at the computer: “I will fucking stab you.”

In 15 minutes’ time, he is due to speak at the inaugural Byline festival, an event designed to champion journalism, freedom of speech and diversity – “Woodstock for the Facebook generation”, as the organisers put it. Love is not here to discuss his legal case, but the recent [WannaCry hacking attack](https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom), in which organised criminals sought to hold to ransom hundreds of thousands of computers – including some belonging to the NHS – in more than 150 countries.

His laptop, however, is not playing along. Love is typically gentle and affable, bright-spoken and witty. (“What’s in your bag outside,” I asked, the first time we met. “State secrets,” he replied, without missing a beat.) But in the oncoming glare of this public speaking engagement, frustration has curdled into rage. His long-term girlfriend, the fashion model Sylvia Mann, leans over, places a hand on Love’s shoulder and softly helps him. Love settles back into his seat, calmed.



*Lauri Love in September 2016. Photograph: Technomage Industries/Courage Fo/PA*

His speech, the first of the festival, is delivered to a smattering of an audience. Love speaks confidently. Afterwards, he and Mann share a minute-long embrace in the front row, while someone fetches him a congratulatory beer. It’s clear that Love’s appearance here is part of a campaign to show himself to be a useful asset to his country. Love was one of a group of British hackers and computer scientists who worked around the clock to disarm the WannaCry attack. He tells me that he is now considering setting up a social enterprise scheme to steer bright, young, web-savvy people away from digital vandalism towards more productive pursuits. “I wasted my youth on the internet,” he says. “I need to somehow harness that experience so others don’t. I want to be able to make a contribution to society.”

There is a moral hazard to hacking young, he says. “The internet distances you from the effects of your actions.” The internet also distances us from ideas of national borders, laws and sovereignty. Should a criminal be prosecuted in the country in which a website is browsed, or the country in which the website is hosted? “The internet isn’t borderless,” says Lewis. “It’s an illusion created by the speed of connectivity. The internet lets you commit a crime in one country while living in another, but it’s still a crime. The practice under international law is that the accused should face trial in the country where they committed the crime.” Todner, who successfully fought McKinnon’s extradition, disagrees, stating simply: “He was in this country when any crime may have been committed.”

Harnessing this generation rather than criminalising it is, Love believes, the key to defending ourselves from the gathering deluge of cybercrime. Since his name was made public, Love tells me that he has been approached “more times than I care to remember” by criminal groups asking if he would help them hack a bank, or skim a cashpoint. “We’re at the point now where lives are at risk because of insecurity,” he says, referring to the WannaCry attack. The argument for countries to find a way, where possible, to enlist hackers rather than prosecute them is a persuasive one, especially when governments lack funding to fight cybercrime as well as knowledge about where best to deploy their limited funds.

It is a position shared by Davis, a friend of Love’s and a former hacker associated with Anonymous, who was arrested in 2011 for targeting Sony, the CIA, the UK’s Serious Organised Crime Agency and News International. (He replaced the Sun’s homepage with a fake story claiming Rupert Murdoch had died.) “Lauri is ridiculously talented,” says Davis, who served just 38 days in a young offender’s institute for his attacks on US computer networks. “The word that keeps coming to mind throughout this whole ordeal is ‘waste’. It’s such a waste of time, money and effort to attempt to extradite him, and an even bigger waste of talent.”

But there is little reason to believe that the British or US governments are likely to heed Davis’s advice. Last month, the US arrested the [23-year-old British IT expert Marcus Hutchins](https://www.theguardian.com/technology/2017/aug/11/marcus-hutchins-arrested-wannacry-kronos-cybersecurity-experts-react) while he was attending an annual hacker conference in Las Vegas, accusing him of helping to design a piece of malware two years ago. Hutchins, who became famous for finding the “kill switch” that defused the WannaCry attack, denies all the charges against him. But according to a report in the Times, GCHQ knew that Hutchins was under US investigation and, in taking a plane to North America, had flown into a trap. One source stated that the FBI waited until Hutchins was on US soil before attempting to make an arrest – precisely to avoid the kind of lengthy extradition battle in which Love is embroiled.

As Love drinks a beer from a plastic cup outside the tent where he gave his speech, I ask him what the best outcome for all of this might be.

“We avert an ecological crisis and humanity still has a civilisation in 100 years?” he says, with a smile.

“Unlikely,” I say. “No, for you, I mean?”

“I often think about how I would kill myself,” he says, after a moment. “Maybe I’ll jump in front of that bus? So I have to concentrate on understanding that there is a beneficial purpose to my going through this. People died for the legal rights and protections we enjoy in the UK. People died for the right to not be held up pending your trial. People died fighting for the right to see the evidence.”

• Follow the Long Read on Twitter at [@gdnlongread](https://twitter.com/%40gdnlongread), or sign up to the long read weekly email [here](https://www.theguardian.com/info/ng-interactive/2017/may/05/sign-up-for-the-long-read-email).